

AB:PP

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICE ASSIGNED WITH
CALL NUMBER (843) 278-1750 AND IMEI
NUMBER 015423000048550, THAT IS IN
THE CUSTODY OR CONTROL OF
CENTURYLINK

TO BE FILED UNDER SEAL

**APPLICATION FOR A SEARCH
WARRANT FOR PROSPECTIVE CELL
SITE INFORMATION**

Case No. 20-MJ-57

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Elisabeth Wheeler, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular device assigned with CALL NUMBER (843) 278-1750 AND IMEI NUMBER 015423000048550 ("the SUBJECT ACCOUNT"), with listed subscribers not known, that is in the custody or control of CenturyLink, a wireless communications provider that is headquartered at 600 New Century Parkway New Century, KS 66031. As a provider of wireless communications service, CenturyLink is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15).

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require CenturyLink to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

3. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” see 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. See 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. See 18 U.S.C. § 3123(b)(1).

4. I am a Special Agent with the Federal Bureau of Investigation, and have been for the past eight years. As a result of my training and experience, I have conducted or participated in the execution of search warrants, including analysis of cellphone location data. Thus, I have experience using various forms of electronic surveillance to locate and apprehend subjects.

5. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file, including the defendant’s criminal history record; and from reports of law enforcement officers involved in the investigation. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that Gerod Woodberry has violated 18 U.S.C. § 2113(a) (bank robbery). As set forth in more detail below, Woodberry was charged with these crimes on January 14, 2020 and is the subject of an arrest warrant issued on that same day. There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting Woodberry, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

7. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. The United States, including Federal Bureau of Investigation, is conducting a criminal investigation of Gerod Woodberry regarding possible violations of 18 U.S.C. § 2113(a) (bank robbery).

9. On January 8, 2020, Gerod Woodberry was arrested by the New York City Police Department (“NYPD”) for a robbery that occurred on December 30, 2019, and he subsequently released without bail. Prior to his release, a Detective with the NYPD asked Woodberry for the phone number of the phone in his possession and Woodberry provided the phone number for the SUBJECT ACCOUNT. The Detective then examined the exterior of the phone and physical SIM Card, and determined the IMEI number for this phone. Law enforcement has not yet been able to confirm from the provider the subscriber name and address for this phone number.

10. On January 10, 2020, Woodberry committed another bank robbery after he was released. On January 14, 2020, this Court authorized the arrest of Gerod Woodberry for a violation of Title 18, United States Code, Section 2113(a) based on the January 10, 2020 robbery. *See* 20-MJ-52.

11. Law enforcement has been attempting to locate Gerod Woodberry since January 10, 2020, and has been unable to determine his location and arrest him. Accordingly, I seek authorization for a prospective cell-site warrant so that law enforcement may locate Gerod Woodberry and arrest him for the violation of 18 U.S.C. § 2113(a).

12. In my training and experience, I have learned that CenturyLink is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

13. Based on my training and experience, I know that CenturyLink can collect cell-site data on a prospective basis about the SUBJECT ACCOUNT. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as CenturyLink typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

14. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Equipment Identity (“IMEI”). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication’s content. Currently, the SUBJECT PHONE has IMEI Number 015423000048550.

15. Based on my training and experience, I know that wireless providers such as CenturyLink typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as CenturyLink typically collect and retain information about their subscribers’ use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT ACCOUNT’s user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

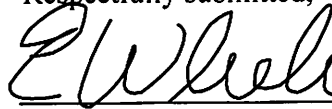
16. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. The proposed warrant will also function as a pen register order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and/or trap and trace device to record, decode, and/or capture certain information in Attachment A for each communication to or from the SUBJECT ACCOUNT, without geographic limit, for a period of forty-five days (45) days pursuant to 18 U.S.C. § 3123(c)(1).

17. I further request that the Court direct CenturyLink to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on CenturyLink, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

18. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving

targets an opportunity to destroy or tamper with evidence, change patterns of behavior, and flee from prosecution.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read 'Elisabeth Wheeler', written over a horizontal line.

Elisabeth Wheeler
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 16, 2020

✓

HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular device assigned CALL NUMBER (843) 278-1750 AND IMEI NUMBER 015423000048550 (“the SUBJECT ACCOUNT”), that is in the custody or control of CenturyLink, a wireless communications provider that is headquartered at 600 New Century Parkway New Century, KS 66031.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following information about the customers or subscribers associated with the SUBJECT ACCOUNT for the time period December 1, 2019 – present.
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and

- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. Information associated with each communication to and from the SUBJECT

ACCOUNT for a period of 45 days from the date of this warrant, including:

- i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
- ii. Source and destination telephone numbers;
- iii. Date, time, and duration of communication; and
- iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the SUBJECT PHONE will connect at the beginning and end of each communication.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 2113(a) (bank robbery) involving Gerod Woodberry during the period December 1, 2019 – present.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.